

Dkt. 61002

REMARKS

Claims 1-14 remain in the application, with independent claim 1 having been amended hereby.

The claims have been carefully reviewed and amended with particular attention to the points raised in the Office Action. It is submitted that no new matter has been added and no new issues have been raised by the present amendment.

Reconsideration is respectfully requested of the rejection of claim 1 under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the written description requirement.

Claim 1 has been amended hereby to address the instance noted in the Office Action.

Withdrawal of the rejection of claim 1 under 35 U.S.C. § 112, first paragraph, is respectfully requested.

Reconsideration is respectfully requested of the rejection of claim 1 under 35 U.S.C. § 103(a), as allegedly being unpatentable over J. Clark et al., "A Survey of Authentication Protocol Literature: Version 1.0," (1997) (hereinafter "Clark et al.")).

Applicants have carefully considered the comments of the Office Action and the cited reference, and respectfully submit that amended independent claim 1 is patentably distinct over the cited reference for at least the following reasons.

The present invention relates to a method and apparatus for mutual authentication of components in a network using a challenge-response method. At least one data pair including a first random number and a first response are requested from an

Dkt. 61002

authentication center. The first random number is passed to a terminal which uses an internally stored key and the first random number to calculate the first response.

The calculated first response is sent to the network, and a second response calculated in the authentication center is sent in response to a second random number. The first response sent from the terminal to the network is used as the second random number. The network has previously requested the second response from the authorization center together with the first random number and the first response as a triplet data set.

Clark et al., as understood by Applicants, relates to a compendium of information related to authentication, including cryptographic prerequisites, protocol types, attacking authentication protocols, methods for analysis of authentication, and a protocol library.

The Office Action cites section 6.3.1 of Clark et al. as allegedly disclosing a method comprising, inter alia, a step of passing the first random number (Challenge 1) to the terminal which uses an internally-stored key and the first random number to calculate the first response (Response 1) (see Office Action, p. 4, lns. 3-17). The Office Action further states that "[t]his challenge is a random number since keys are random numbers ..." (see id.). Applicants respectfully disagree.

As understood by Applicants, the cited section of Clark et al. relates to symmetric key protocols involving trusted third parties, and specifically to the Needham Schroeder

Dkt. 61002

Protocol with conventional keys (see Clark et al., pp. 46-47). In the third step of the protocol, $A \rightarrow B : E(K_{bs} : K_{ab}, A)$, A sends to B the encrypted message component obtained from the server (see id.; p. 19, lns. 1-30).

It is respectfully submitted, however, that an encryption key (e.g., K_{ab}) is not equivalent to a random number (e.g., N_b). An encryption key is a predefined and specific numeric value which is used for a certain period of time and which is not changed during the period of time. The key cannot be randomly selected as it must be known to both terminal and network.

In contrast, a random number is a randomly-selected number used, for example, as a Challenge value in an authentication procedure. Different random numbers may be used for each authentication procedure performed.

Furthermore, it is respectfully submitted that the protocol described in the cited section of Clark et al. does not disclose the mutual authentication method recited in the present invention.

As understood by Applicants, the method set forth in section 6.3.1 of Clark et al. includes five messages (see Clark et al., p. 19, lns. 2-28; p. 46, lns. 21-29).

In message (1), server S sends a key to A upon request, and includes nonce N_a (see id.).

Message (2) is sent from S to A, and includes an encrypted message E which is encrypted with key K_{as} . K_{as} is known only to A and S, and message E includes random number N_a , identifier B, key K_{ab} , and encrypted message B including

pkt. 61002

key K_{ab} and identifier A encrypted with key K_{bs} (see id.).
Message E cannot be decrypted by A because it does not know
key K_{bs} .

Message (3) is sent from A to B and is encrypted with key
 K_{bs} and includes key K_{ab} and identifier A (see id.). No
random number (Challenge) is included in this message.

In message (4), B sends random number N_b (Challenge 1),
encrypted with key K_{ab} , to A (see id.).

In message (5), A sends a response (Response 1) having a
value of (N_b-1) to B, encrypted with key K_{ab} (see id.).

It is respectfully submitted, however, that the method of
the cited section of Clark et al. does not disclose or suggest
the use of two challenge values and two response values for
authentication, as recited in amended independent claim 1.

In contrast, in the mutual authentication method of the
present invention, as recited in amended independent claim 1,
at least one data pair including a first random number
(Challenge 1) and a first response (Response 1) are requested
from an authentication center using a request from the
network. The first random number (Challenge 1) is passed to
the terminal which calculates the first response (Response 1)
based upon an internally stored key and the first random
number (Challenge 1), and the calculated first response
(Response 1) is sent to the network. The network responds to
a second random number with a second response (Response 2)
calculated in the authentication center, wherein the first
response (Response 1) sent from the terminal to the network is
also used as the second random number (Challenge 2), and

Dkt. 61002

whereby the network has previously requested the second response (Response 2) from the authentication center together with the first random number (Challenge 1) and the first response (Response 1) as a triplet data set (Challenge 1/Response 1/Response 2).

Furthermore, it is respectfully submitted that the above-described method of Clark et al. does not disclose or suggest that the first response corresponds to the first random number.

In contrast, in the present invention, the first random number (Challenge 1) is passed to the terminal, and the terminal calculates the first response (Response 1) based upon an internally stored key and the first random number (Challenge 1), as recited in amended independent claim 1.

Additionally, in the present invention, the first response (Response 1), calculated in the terminal and sent from the terminal to the network, is used as the second random number (Challenge 2). The network is not required to send another random number to the terminal. The required random number (Challenge 2) is available in the terminal, as it corresponds to the first response (Response 1) which has been calculated by the terminal (see specification of the present application, p. 4, lns. 11-19).

That is, in the present invention, the terminal does not produce the second random number (Challenge 2), but equates it to the second response (Response 2) (see id., p. 4, ln. 20 to p. 4a, ln. 5). The network can thus produce a second response and send it to the terminal, which compares it to the value in

Dkt. 61002

the terminal to determine if the network is authentic (see id.).

It is respectfully submitted that neither the cited section, nor the remainder, of Clark et al. disclose or suggest a method for mutual authentication of components in a network comprising the steps of requesting at least one data pair including a first random number and a first response from an authentication center using a request from the network, passing the first random number to the terminal which calculates the first response based upon an internally stored key and the first random number, sending the calculated first response to the network, and responding to a second random number with a second response calculated in the authentication center, the response performed by the network, wherein the first response sent from the terminal to the network is also used as the second random number, whereby the network has previously requested the second response from the authentication center together with the first random number and the first response as a triplet data set, as described above and as recited in amended independent claim 1.

Accordingly, for at least the above-stated reasons, it is respectfully submitted that independent claim 1, and the claims depending therefrom, including claims 2-14, are patentable over the cited reference.

Withdrawal of the rejection of claim 1 under 35 U.S.C. § 103(a) is respectfully requested.

Reconsideration is respectfully requested of the rejection of claims 2-14 under 35 U.S.C. § 103(a), as

Dkt. 61002

allegedly being unpatentable over Clark et al. in view of U.S. Patent No. 5,544,245 to Tsubakiyama.

Applicants have carefully considered the comments of the Office Action and the cited references, and respectfully submit that claims 2-14 are patentably distinct over the cited references for at least the following reasons.

Tsubakiyama, as understood by Applicants, relates to a mutual authentication/cipher key delivery system in which a communication network and all of its users have devices for implementing a common key cryptosystem. Identifier ID_i of user i is made public in the network. An authentication key K_i of user i is known only to the network and the user, and each user generates a random number r_n for authentication of the network and sends it and his identifier ID_i to the network.

The network inputs into a specific function $F()$ the random number r_n received from the user and a random number r_u generated by the network itself, encrypts the resulting output value $F(r_n, r_u)$ by an encryption algorithm $ElK_i()$ using the authentication key K_i of the individual user as a cipher key and sends the encrypted data C_i to the user. The user obtains D_i by inputting the data C_i into inverse function $ElK_i^{-1} K_i()$ of the encryption algorithm $ElK_i()$ using the user's authentication key K_i as a cipher key, inputs D_i into an inverse function $F^{-1}()$ of the function $F()$, and judges the network to be valid only when d_i is equal to the random number r_n . This is completely different from the present method.

It is respectfully submitted that amended independent claim 1, and the claims depending therefrom, including claims

Dkt. 61002

2-14, are patentable over Clark et al. for at least the reasons set forth above.

It is respectfully submitted, therefore, that neither Clark et al. nor Tsubakiyama, alone or in combination, disclose or suggest a method for mutual authentication of components in a network comprising the steps of requesting at least one data pair including a first random number and a first response from an authentication center using a request from the network, passing the first random number to the terminal which calculates the first response based upon an internally stored key and the first random number, sending the calculated first response to the network, and responding to a second random number with a second response calculated in the authentication center, the response performed by the network, wherein the first response sent from the terminal to the network is also used as the second random number, whereby the network has previously requested the second response from the authentication center together with the first random number and the first response as a triplet data set, as described above and as recited in amended independent claim 1.

Accordingly, for at least the above-stated reasons, it is respectfully submitted that independent claim 1, and the claims depending therefrom, including claims 2-14, are patentable over the cited references.

Withdrawal of the rejection of claims 2-14 under 35 U.S.C. § 103(a) is respectfully requested.

Should the Examiner disagree, it is respectfully requested that the Examiner specify where in the cited

Dkt. 61002

document there is a basis for such disagreement.

Entry of this amendment is earnestly solicited, and it is respectfully submitted that this amendment raises no new issues requiring further consideration and/or search, because the functional aspects of the invention have merely been clarified in the amended claims.

The Office is hereby authorized to charge any fees which may be required in connection with this amendment and to credit any overpayment to Deposit Account No. 03-3125.

Favorable reconsideration is earnestly solicited.

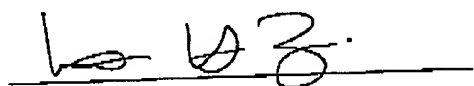
Respectfully Submitted,

Dated: July 7, 2004

I hereby certify that this correspondence is being facsimile transmitted on this date to the U.S. Patent and Trademark Office (Fax. No. (703) 872-9306).

Norman H. Zivin
Reg. No. 25,385

Date


Norman H. Zivin
Reg. No. 25,385
c/o Cooper & Dunham LLP
1185 Avenue of the Americas
New York, NY 10036
(212) 278-0400
Attorney for Applicants